UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

U.S. DISTRICT COURT
EASTERN DISTRICT-WI
GREEN BAY DIV.

'09 OCT -5 P12:46

FILED
JON W. SANFILIPPO
CLERK

In the Matter of the Search of

the premises known as:
The residence located at 1621 Eleventh Avenue, in the City of Green Bay, Brown County, Wisconsin, in the State and Eastern District of Wisconsin and more particularly described as a one-story residence with reddish brown brick siding and white trim. The numbers "1621" are displayed above the front door of the residence. There is a detached one-car garage with brick siding.

Application & Affidavit
For Search Warrant
Case No. 09 M 649

I, Patrick Lynch, being duly sworn depose and say: I am a Special Agent for the Federal Bureau of Investigation, and have reason to believe that on the property or premises known as the residence located at 1621 Eleventh Avenue, in the City of Green Bay, Brown County, Wisconsin, in the State and Eastern District of Wisconsin and more particularly described as a one-story residence with reddish brown brick siding and white trim. The numbers "1621" are displayed above the front door of the residence. There is a detached one-car garage with brick siding.

in the Eastern District of Wisconsin, there is now concealed certain property, namely: See Attachment A- Items To Be Searched For and Seized, which is **the evidence of crime, contraband, and fruits of crime,** concerning violations of Title 18 United States Code, Sections 2252 and 2252A.

The facts to support a finding of Probable Cause are as follows:

See the attached affidavit of Special Agent Patrick Lynch

Continued on the attached sheet and made a part hereof. √ Yes _No

Patrick Lynch
Signature of Affiant
PATRICK LYNCH

Sworn to before me, and subscribed in my presence

October 5, 2009 12:30 PM
Date and time issued

at Green Bay, Wisconsin
City and State

Hon. James R. Sickel, U.S. Magistrate Judge
Name & Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Patrick Lynch, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent (SA) with the FBI since 1987, and am currently assigned to the Green Bay Resident Agency (GBRA), located in the Eastern District of Wisconsin. Since joining the FBI, I have investigated violent crimes, white collar crimes, computer crimes, and crimes involving the sexual exploitation of children (SEOC). I have also spoken to other knowledgeable agents, attended seminars, and attended classes on such investigations.

2. I began investigating SEOC cases in approximately 1997. I have received specialized instruction in the area of child pornography investigations. The training included learning the characteristics of child pornographers and successful computer investigations related to child pornography. That training has continued to the present.

3. I have participated in more than twenty child pornography investigations. This includes obtaining and executing search warrants, interviewing subjects and targets, assisting in evidence collection, and analyzing evidence from forensic examinations.

4. My training and experience has allowed me to become familiar with the methods used by child pornographers to receive, collect, and distribute child pornography, and the manner in which they communicate with the sellers, distributors, and suppliers of child pornography.

PURPOSE OF THE AFFIDAVIT

5. I am investigating the activities of a person or persons who reside at 1621 Eleventh Avenue, in the City of Green Bay, in the State and Eastern District of Wisconsin. Based upon the evidence developed to this point, there is probable cause to believe that a person or persons at this residence, received, possessed, and transmitted child pornography, in violation of Title 18, United States Code,

Sections 2252 and 2252A, and that there is evidence of such crimes at the residence. I am requesting a search warrant for the Eleventh Avenue residence (hereinafter referred to as the "Premises"), more particularly described in paragraph 33 below, for the items specified in Attachment A. I request authority to search the Premises, including any assigned storage areas or garages, and any computer and computer media located therein, where the items specified in Attachment A may be found, and to seize all such items as instrumentalities, fruits, and evidence of crime.

6. This affidavit is based not only on my own training, experience, and investigation, but also on information provided by FBI Special Agent Joseph M. Cecchini and Time Warner Cable.

STATUTORY AUTHORITY

7. This investigation concerns alleged criminal SEOC violations of Title 18, United States Code, Sections 2252 and 2252A.

a. 18 U.S.C. § 2252(a) prohibits anyone from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

b. 18 U.S.C. § 2252A(a) prohibits anyone from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was

either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

c. 18 U.S.C. § 2252(a)(1) prohibits anyone from knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct.

d. 18 U.S.C. § 2252(a)(2) prohibits anyone from knowingly receiving or distributing, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct that has been mailed or shipped or transported in interstate or foreign commerce. That subsection also makes it a crime for any person to knowingly reproduce any visual depiction of minors engaging in sexually explicit conduct for distribution in interstate or foreign commerce by any means, including by computer or the mail.

e. 18 U.S.C. § 2252(a)(4) prohibits anyone from possessing one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce or that were produced using materials that had traveled in interstate or foreign commerce.

f. 18 U.S.C. § 2252A(a)(1) prohibits anyone from knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.

g. 18 U.S.C. § 2252A(a)(2) prohibits anyone from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

h. 18 U.S.C. § 2252A(a)(3) prohibits anyone from knowingly possessing reproducing child pornography for distribution through the mail or in interstate or foreign commerce by any means, including by computer.

i. 18 U.S.C. § 2252A(a)(5)(B) prohibits anyone from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

DEFINITIONS

8. The following definitions apply to this affidavit:

a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors, but that do not meet the definition of child pornography or sexually explicit conduct.

b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been

created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct. *See* 18 U.S.C. §§ 2252, 2256(2), and 2256(8).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

e. "Computer" is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer hardware" consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and

diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software" is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which preform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Internet Protocol address," a/k/a "IP address," refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the user's Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

k. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

9. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced

using film cameras, and took the form of still photography or movies. The undeveloped photographs and films required darkroom facilities and skill to produce the images. There were definable costs involved with the production of pornographic images, and any relatively large-scale distribution of these images required significant resources. The photographs required sufficient and secure storage to maintain them and to prevent their public exposure. Their distribution was typically accomplished through a combination of personal contacts, mailings, and telephone calls.

10. This type of distribution scheme has been dramatically changed by computers and the Internet, which combine to serve four basic functions in connection with child pornography: production, storage, communication, and distribution.

11. Child pornographers can now transfer film photographs to a computer with a device known as a scanner, and digital cameras allow the captured images to be transferred directly to a computer. A modem allows a computer to connect to another computer through the use of telephone, cable, or wireless connection. The necessary hardware to accomplish these tasks - a computer, a scanner, a digital or film camera, a modem, and an Internet connection - are relatively inexpensive and readily available to the public. Using this hardware and widely available software, millions of computer users around the world can quickly and easily store and distribute electronic digital information, including child pornographic images.

12. The computer's ability to store digital images makes the computer an ideal repository for child pornography. The home computer's storage capacity, including the hard drive and external storage devices (zip drives, thumb drives, etc.), has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

13. Not only can collectors and distributors of child pornography use their own computer to store child pornography images, they can also use online resources to do so, including services offered by Internet Portals such as Google, Yahoo!, Hotmail, and others. These online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even when a child pornographer uses this type of web-based storage, a forensic examiner can often find evidence of the online storage on the user's computer.

14. The Internet and its World Wide Web afford child pornography collectors different methods for obtaining, viewing, and trading child pornography in a relatively instantaneous, secure, and anonymous fashion. Common methods of communication and file sharing/retrieval include visiting web pages, sending e-mail, using instant messenger (IM) programs to engage in real-time chats with other users and to share digital images during the chats, and using peer-to-peer (P2P) programs to search the shared folders of other users for desired images.

15. Evidence of computer communications is often stored on the user's computer. Storing this information can be intentional – e.g. by saving an IM chat or an e-mail in a designated location, or by saving one's favorite websites. Digital information can also be stored unintentionally – e.g. traces of the path of an internet search, e-mail, or IM may be automatically stored by internet browser software, e-mail software, IM software, or ISP client software. A forensic examiner can retrieve this stored information. A forensic examiner can also determine whether the computer contains, or did contain, these types of software even if no child pornography images remain on the system. Such information is often maintained indefinitely until overwritten by other data.

BACKGROUND ON PEER-TO-PEER PROGRAMS

16. A widely used form of digital information sharing available to Internet users is called peer-to-peer (P2P) and is accomplished through the use of special software. The software is designed to allow hundreds, thousands, or even millions of Internet users to trade digital files through a user network. There are several P2P networks currently operating, and Gnutella is one of the most popular. There are several different P2P software applications, including Limewire, that can be used to access Gnutella's network. Gnutella works differently than traditional searches and navigation on the Internet's world wide web. Traditional web surfing involves accessing data that is stored, or hosted, on a known central server. Gnutella's P2P network, on the other hand, utilizes "nodes" that allows Limewire users to search for and directly access each others' computers for desired digital files. Gnutella's network is often referred to as a "server-client" structure, because each individual user is not only a client (i.e. looking for files), it can also serve as a server (i.e. providing files to others). As stated on the Limewire web site, "Gnutella is not a web site. It doesn't contain web sites. The content that is available on the Gnutella Network does not come from websites or from the publishers of Gnutella-compatible software; it comes from other users running Gnutella-compatible software on their own computers."

17. While the technology behind Limewire may be complex, obtaining and using it is not. Limewire maintains a website where a user can download the Limewire software for free in one of fourteen different languages. Limewire refers to itself as the "fastest file sharing program on the planet," allowing users to share digital picture and movie files. Limewire's stated goal is to "build users a tool that allows them to easily publish content to the world." After the download, Limewire is then a program file on the individual's computer. Limewire allows the user to set up folders on

the user's computer which contain image files to be shared with others running Limewire. When the Limewire software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's shared folder can be downloaded by other Limewire users in the network. Most P2P software, including Limewire, encourage file sharing to propagate the network. The more files a user is sharing, the greater his/her ability is to download files. However, a user is not required to keep files in the shared folder, or to share files to utilize the P2P network. A Limewire user can easily open his/her shared folder to see which files are there, and move or delete those files to keep others from accessing them.

18. A Limewire user obtains files by opening the software on the user's computer, and conducting a search for desired files that are currently being shared on the network. Limewire uses keyword searches, and the search results are displayed to the user. The user then selects file(s) from the results for download. The file download is achieved through a direct connection between the computer requesting the file and the computer containing the file.

19. For example, a Limewire user interested in obtaining child pornographic images would open the Limewire application on his/her computer and conduct a search for files using a term such as "preteen sex." The search is sent out over the network of computers running Limewire at that moment, and looks at the "shared" folders of those other Limewire users for files that match the search term. The search results are returned to the user's computer and displayed. The user selects the file(s) he/she wants to download. The file(s) is/are downloaded directly from the computer hosting the file(s). The downloaded file(s) is/are stored in the area previously designated by the user. The downloaded file will remain there until moved or deleted.

20. One advantage to P2P file sharing is that multiple files may be downloaded in parallel, allowing the user to download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time, which speeds up the time it takes to download the file. Thus, a Limewire user downloading an image file may actually receive parts of the image from multiple computers. Often, however, a Limewire user receives the entire image from one computer.

21. As with all Internet connections, a P2P file transfer is assisted by reference to an IP address. This address is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

BACKGROUND OF THE INVESTIGATION

22. The following investigative information has been relayed to me by FBI SA Joseph M. Cecchini, an Online Covert Employee. SA Cecchini provided a written report documenting his investigation.

23. On July 27, 2009, SA Cecchini connected to the internet in an on-line undercover capacity. He signed onto the Peer-to-Peer file sharing program Limewire. SA Cecchini used screen capture software to capture image and video file listings. SA Cecchini utilized the Freeware version of Limewire, which has been enhanced to limit downloads from a single source. Additionally, the software has an embedded mechanism that logs the traffic between the undercover computer and the target computer.

24. While online, SA Cecchini performed a file query using the search term "childfugga," which is known to be associated with child pornography image files. The search included a response from Internet Protocol (IP) address 24.166.149.215.

25. SA Cecchini executed a browse user command for the individual using IP address 24.166.149.215 and subsequently was able to connect with this IP address and obtain a list of files this user was sharing.

26. SA Cecchini viewed the list of files available from IP address 24.166.149.215. The list contained 109 files with names consistent with child pornography. SA Cecchini subsequently initiated several downloads from the files listed.

27. During SA Cecchini's undercover session, identified as UOC-11723, he downloaded 42 image files from a P2P user who was assigned IP address 24.166.149.215.

28. The Maxmind IP database is a publicly-available Internet resource that tracks the assignment of IP addresses to Internet Service Providers (ISPs). It has proven to be a reliable source. SA Cecchini accessed the Maxmind database to learn that the IP address 24.166.149.215 was among a set of IP addresses assigned to ISP Time Warner Cable/Road Runner. SA Cecchini served an administrative subpoena on Road Runner seeking the subscriber and billing information for IP address 24.166.149.215 for Session UOC-11723 on July 27, 2009, from 11:04 CDT to 11:16 CDT.

29. The parent company of Road Runner, Time Warner Cable, responded to the subpoena. I requested clarified information on September 28, 2009 regarding the subpoena. Time Warner Cable indicated that for the requested date and time, the IP address 24.166.149.215 had been assigned to an account holder named Jason R. Quinn, with an address of 1621 Eleventh Avenue, Green Bay, Wisconsin 54304-3614, and email addresses of jquinn6@new.rr.com.

30. I have reviewed the images downloaded by SA Cecchini in undercover session UOC-11723 from IP address 24.166.149.215. Some of the file names and images are described as follows:

Filename	Description
hornytoad's best cp ptn lsm pthc (219).jpg	A prepubescent female engaged in sexual intercourse with an adult male.
hornytoad's best cp ptn lsm pthc (245).jpg	An adult female inserting a vibrator into the vagina of a prepubescent female.
hornytoad's best cp ptn lsm pthc (220).jpg	A prepubescent female engaged in oral sex with an adult male.
hornytoad's best cp ptn lsm pthc (214).jpg	A prepubescent female engaged in oral sex with an adult male.
hornytoad's best cp ieen daughter ptn lsm pthc (1)(1).jpg	A prepubescent female engaged in oral sex with an adult male.

31. I have received a copy of these images noted above that were downloaded by SA Cecchini. I believe all these image files meet the statutory definition of sexually explicit conduct.

32. I have further queried the rercords from the Wisconsin Department of Transportation. Those records indicate that Jason R. Quinn (d.o.b. 11/14/1972) holds an active drivers license and currently lists his residence at 1621 Eleventh Avenue, Green Bay, Wisconsin.

DESCRIPTION OF THE PREMISES

33. On September 1, 2009, I conducted surveillance at 1621 Eleventh Avenue, Green Bay, Wisconsin, which is located in Brown County, in the State and Eastern District of Wisconsin, and hereinafter referred to as the Premises. The Premises are more particularly described as follows:

> The residence is located on the northeast corner of Eleventh Avenue and Liberty Street. It is a one-story residence with reddish brown brick siding and white trim. The numbers "1621" are displayed above the front door of the residence. There is a detached one-car garage with brick siding.

COMPUTER SEARCHES AND SEIZURES

34. Computer searches and seizures commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an

operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

c. A forensic computer examination can recover files and remnants of files months or even years after they were obtained. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person deletes a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files viewed over the Internet are automatically downloaded into a temporary Internet directory or "cache' Files in the cache are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

35. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

36. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251 through 2256, and should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

37. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

38. Based on my training and experience, I know that collectors of child pornography exhibit certain common characteristics. I have consulted in the past with other FBI Special Agents who have investigated child pornography cases out of both the Green Bay Division and the Milwaukee Division of the FBI. I have also consulted in the past with Supervisory Special Agent (SSA) Jennifer Eakin in the Federal Bureau of Investigation. SSA Eakin has been a Special Agent since 1984 and is now assigned to the Behavioral Analysis Unit at the FBI Academy in Quantico, Virginia where she consults on a daily basis with both foreign and domestic police agencies on Crimes Against Children, and particularly on behavioral issues associated with the Internet Sexual Exploitation of Children. She is a qualified expert in this field and has testified as such in federal court. In addition, SSA Eakin is involved in the following ongoing research projects focusing on the Internet Offender: a joint project with the Federal Bureau of Prisons examining the relationship between collecting child pornography and hands-on offending; and an archival review of closed cases addressed by the FBI's Innocent Images Undercover Initiative focusing on the behavior of online child sex offenders.

39. According to SSA Eakin, most individuals who collect child pornography are sexually attracted to children, their sexual arousal patterns and erotic imagery focus, in part or in whole, on children. The collection may be exclusively dedicated to children of a particular age/gender or it may be more diverse, representing a variety of sexual preferences, including children. Child pornography collectors express their attraction to children through the collection of sexually explicit materials involving children as well as other seemingly innocuous material related to children.

These individuals may derive sexual gratification from actual physical contact with children as well as from fantasy involving the use of pictures or other visual depictions of children or from literature describing sexual contact with children. The overriding motivation for the collection of child pornography may be to define, fuel, and validate the collector's most cherished sexual fantasies involving children. Visual depictions may range from fully clothed depictions of children engaged in non-sexual activity to nude or partially nude depictions of children engaged in explicit sexual activity. In addition to child pornography, these individuals are also highly likely to collect other paraphernalia related to their sexual interest in children. This other material is sometimes referred to as "child erotica" which is defined as any material, relating to children, that serves a sexual purpose for a given individual. It is broader and more encompassing than child pornography, but at the same time the possession of such corroborative material, depending on the context in which it is found, may be behaviorally consistent with the offender's orientation toward children and indicative of his intent. It includes things such as fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, cartoons and non-sexually explicit visual images.

40. According to SSA Eakin, child pornography collectors reinforce their fantasies, often by taking progressive, overt steps aimed at turning the fantasy into reality in some or all of the following ways: collecting and organizing their child-related material; masturbating while viewing the child pornography; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other like-minded adults through association with groups catering to their sexual preference for children thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities and/or relationships which provide access or proximity to children; and

frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self interest.

41. SSA Eakin advised that child pornography collectors almost always maintain and possess their material in the privacy and security of their homes or some other secure location where it is readily available. The collection may include sexually explicit or suggestive materials involving children, such as photographs, magazines, narratives, motion pictures, video tapes, books, slides, drawings, computer images or other visual media. The collector is aroused while viewing the collection and, acting on that arousal, he often masturbates thereby fueling and reinforcing his attraction to children. This is most easily accomplished in the privacy of his own home. Because the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished sexual fantasies, the collector rarely, if ever, disposes of the collection. Even if the collector feels threatened, he will usually seek to preserve the collection by hiding it better rather than destroying the material. The collection may be culled and refined over time, but the overall size of the collection tends to increase. In fact, many collectors protect their collections by creating back-ups, sometimes multiple back-ups, of some or all of the collection. Child pornography, unlike some other kinds of contraband (e.g. drugs), is not "consumed" by the user. The "consumption" of this product results in its proliferation, more copies are generated. The very nature of computers as a means of collection, transmission, and/or storage lends itself to permanent preservation of the item.

If the collector relocates, his collection almost always moves with him. Individuals who utilize a collection in the seduction of children or to document that seduction treat the materials as prized possessions and are especially unlikely to part with them.

42. The possession of child pornography should be viewed as both a violation of the law and possible corroboration of child sexual victimization. In the context of child molestation, child pornography and child erotica may be used in several ways, including the following: to desensitize or lower the inhibitions of children targeted for seduction; to arouse the selected child partner; and to demonstrate the desired sexual acts. While the collection of child pornography does not tell us what the individual has done or will do, it is the best indicator of what he wants to do.

43. Based on my training and experience, persons who possess images of child pornography are likely to maintain some or all of the images over an extended period of time, ranging from months to years. Based on the specifics of this investigation, including the names of files downloaded by SA Cecchini from the computer associated with the residence of Jason R. Quinn, I believe it is more probable than not that (1) the computer contains contraband in the form of child pornography and (2) such contraband is currently located at 1621 11th Avenue, Green Bay, Wisconsin.

CONCLUSION

44. Based on the above information, there is probable cause to believe that a person or persons who reside at the Premises is/are involved in transmitting, receiving, and possessing child pornography. There is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2225A, as listed in Attachment A, are located on the Premises.

46. I respectfully request that the attached warrant be issued authorizing the search of the Premises and the seizure of the items listed in Attachment A.

Patrick Lynch

PATRICK LYNCH
Special Agent
Federal Bureau of Investigation

Sworn before me this
5 day of October, 2009.

Notary Public, Permanent Commission

ATTACHMENT A

1. Any and all visual depictions of minors that may constitute sexually explicit conduct, child pornography, or child erotica.

2. Computer hardware, software, or electronic storage media that may constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, or other violations related to the sexual exploitation of children.

3. Telecommunications devices or equipment that may constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, or other violations related to the sexual exploitation of children.

4. Cameras, video equipment and other electronic items that may constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, or other violations related to the sexual exploitation of children.

5. Papers or documents that may constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, or other violations related to the sexual exploitation of children.

6. Magazines, books, pictures, videos, or periodicals that may constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, or other violations related to the sexual exploitation of children.

7. Sexual paraphernalia, clothing, or objects that may be evidence of violations of 18 U.S.C. §§ 2252 and 2225A, or other violations related to the sexual exploitation of children.